Listing of the Claims:

This listing of claims replaces all prior versions, and listings, of claims in the application.

1. (previously presented) A method for authenticating a digital medium comprising:

requesting, at a computing device, a read operation of data symbols from a media reading device;

monitoring a transfer rate of read user data from an output of the media reading device to the computing device resulting from the reading of data symbols stored on a digital medium installed on the media reading device at a physical location of the digital medium, wherein the read user data is in a format that can be processed by the computing device and wherein the transfer rate is a rate, in data elements per unit time, at which read user data elements are returned from the media reading device to the computing device in response to the requesting of the read operation;

determining, at the computing device, from the monitored transfer rate, the presence of an anomaly region on the digital medium corresponding to the physical location of the data symbols on the digital medium by identifying a modification in the transfer rate of the read user data from the media device to the computing device; and

authenticating the digital medium based on a characteristic of the anomaly region.

2. (original) The method of claim 1 wherein the digital medium comprises an optical digital medium.

3. (original) The method of claim 1 wherein the digital medium comprises a magnetic digital medium.

4. (previously presented) The method of claim 1 wherein monitoring comprises monitoring

the transfer rate in real time, as the read user data is transferred from the media reading device to the computing device.

5. (previously presented) The method of claim 1 wherein monitoring comprises monitoring the transfer rate following transfer of the read user data from the media reading device to the computing device.

6. (original) The method of claim 1 further comprising estimating the monitored data transfer rate and determining the presence of the anomaly region based on the estimated data transfer rate.

7. (previously presented) The method of claim 1 wherein the anomaly region causes a modification in the transfer rate of the read user data.

8. (previously presented) The method of claim 7 wherein the reading of the data symbols is performed by the media reading device and wherein the modification in the transfer rate results from the media reading device automatically initiating multiple retries of reading the data symbols due to the presence of the anomaly region.

9. (previously presented) The method of claim 7 wherein the reading of the data symbols is performed by the media reading device and wherein the modification in the transfer rate results from the media reading device automatically slowing down the reading of the data symbols due the presence of the anomaly region.

10. (previously presented) The method of claim 1 wherein the anomaly region is located at a predetermined location on the digital medium.

11. (previously presented) The method of claim 10 wherein the predetermined location

comprises an absolute address on the digital medium.

12. (original) The method of claim 11 wherein the absolute address represents an encoded data value.

13. (previously presented) The method of claim 1 wherein the anomaly region is at a location on the digital medium that is analytically determined as a result of the step of determining the presence of the anomaly region.

14. (previously presented) The method of claim 13 wherein the location comprises an absolute address on the digital medium.

15. (original) The method of claim 14 wherein the absolute address represents an encoded data value.

16. (previously presented) The method of claim 1 wherein the anomaly region comprises a first anomaly region and further comprising:

determining, from the monitored transfer rate, the presence of a second anomaly region on the digital medium corresponding to a second physical location of second data symbols on the digital medium; and

wherein a relative location of the second anomaly region is determined relative to the location of first anomaly region.

17. (original) The method of claim 16 wherein authenticating is further based on the determined relative location.

18. (previously presented) The method of claim 16 wherein the second anomaly region is located at a predetermined location on the digital medium.

19. (previously presented) The method of claim 16 wherein the second anomaly region is at a location on the digital medium that is analytically determined as a result of the step of determining the presence of the second anomaly region.

20. (original) The method of claim 16 wherein the relative location represents an encoded data value.

21. (previously presented) The method of claim 1 wherein the characteristic is the location of the anomaly region in the read user data, and wherein if the location of the anomaly region in the read user data matches the physical location of the anomaly region corresponding to the data symbols, then the digital medium is determined as authentic.

22. (previously presented) The method of claim 21 wherein if the location of the anomaly region in the read user data does not match the physical location of the anomaly region corresponding to the data symbols, then the digital medium is determined as non-authentic.

23. (previously presented) The method of claim 1 further comprising controlling user access to the user data read from the digital medium based on whether the digital medium is authentic.

24. (previously presented) The method of claim 23 wherein controlling comprises one of allowing access, disallowing access, and limiting access to the user data read from the digital medium.

25. (previously presented) The method of claim 1 wherein the determination of the presence of the anomaly region results from a difficulty in the reading of the read user data by a reading device.

26. (previously presented) The method of claim 1 wherein the anomaly region comprises a

physical alteration of the digital medium that results in the user data corresponding to the anomaly region being transferred at a transfer rate that is different than a standard transfer rate of user data not corresponding to the anomaly region.

27. (original) The method of claim 26 wherein the physical alteration of the digital medium comprises a mechanical alteration.

28. (original) The method of claim 26 wherein the physical alteration of the digital medium comprises an optical alteration.

29. (original) The method of claim 26 wherein the physical alteration of the digital medium comprises a magnetic alteration.

30. (original) The method of claim 1 wherein the steps for performing the authentication reside in software code that is previously stored on the digital medium, prior to authentication.

31. (original) The method of claim 1 wherein the steps for performing the authentication reside in firmware that is stored in a media drive performing the authentication or in a computing device controlling the media drive, or stored in firmware controlling the media drive, or stored remotely and provided to the media drive by a network connection.

32. (original) The method of claim 1 wherein a known characteristic of the anomaly region is previously stored, prior to authentication, and wherein authenticating the digital medium based on a characteristic of the anomaly region comprises comparing the characteristic to the known characteristic.

33. (canceled).

34. (previously presented) The method of claim 1 wherein the modification in the transfer rate comprises a reduction in the transfer rate and wherein the anomaly region is identified based on the extent of the reduction.

35. (previously presented) The method of claim 1 wherein the modification in the transfer rate comprises a reduction in the transfer rate to a resultant non-zero transfer rate.

36. (original) The method of claim 35 wherein the resultant non-zero transfer rate results in a determination that the anomaly region is a genuine anomaly region.

37. (previously presented) The method of claim 1 wherein the modification in the transfer rate comprises a reduction in the transfer rate to a resultant zero transfer rate.

38. (original) The method of claim 37 wherein the resultant zero transfer rate results in a determination that the anomaly region is a false anomaly region

39. (original) The method of claim 38 wherein the false anomaly region indicates that the digital medium is non-authentic.

40. (previously presented) The method of claim 1 wherein the modification in the transfer rate comprises an increase in the transfer rate, and wherein the characteristic is determined based on the increase.

41. (previously presented) The method of claim 1 wherein the modification in the transfer rate comprises a response comprising an acceptable reduction in the user data transfer rate followed by a sudden increase in the transfer rate to an increased transfer rate that is greater than a maximum transfer rate.

42. (original) The method of claim 41 wherein the response indicates that an apparent anomaly region generated by an external source has been detected.

43. (original) The method of claim 42 further comprising filtering the apparent anomaly region such that authenticating is not based on the apparent anomaly region.

44. (original) The method of claim 1 wherein authenticating is based on a characteristic of multiple anomaly regions.

45. (original) The method of claim 1 wherein authenticating is based on multiple characteristics of the anomaly region.

46. (original) The method of claim 1 wherein the anomaly characteristic comprises anomaly severity.

47. (original) The method of claim 46 wherein the anomaly severity represents an encoded data value.

48. (previously presented) The method of claim 1 wherein monitoring further comprises recording prior settings of the media reading device prior to reading; and restoring the prior settings of the reading device following authenticating.

49. (previously presented) The method of claim 48 wherein, following recording of the prior settings of the media recording device , the media reading device is reset.

50. (previously presented) The method of claim 49 wherein, following recording of the prior settings of the media recording device, a cache on the media reading device is reset.

51. (previously presented) The method of claim 48 further comprising selecting a data block size for the media reading device.

52. (previously presented) The method of claim 48 further comprising disabling excessive retry attempts by the media reading device.

53. (previously presented) The method of claim 48 further comprising reading locations of the digital medium known to be free of anomaly regions in order to determine a maximum transfer rate.

54. (original) The method of claim 48 further comprising ceasing reading when an anomaly location has been encountered.

55. (previously presented) The method of claim 48 further comprising storing the read user data for statistical analysis.

56. (previously presented) A system for authenticating a digital medium comprising:

a computing device that requests a read operation of data symbols from a media reading device;

a monitor that monitors a transfer rate of read user data from an output of the media reading device to the computing device resulting from the reading of data symbols stored on a digital medium installed on the media reading device at a physical location of the digital medium, wherein the read user data is in a format that can be processed by the computing device and wherein the transfer rate is a rate, in data elements per unit time, at which read user data elements are returned from the media reading device to the computing device in response to the requesting of the read operation;

an anomaly detector at the computing device that determines, from the monitored transfer rate, the presence of an anomaly region on the digital medium corresponding to the physical

location of the data symbols on the digital medium by identifying a modification in the transfer rate of the read user data from the media reading device to the computing device; and

an authenticator that authenticates the digital medium based on a characteristic of the anomaly region.

57. (original) The system of claim 56 wherein the digital medium comprises an optical digital medium.

58. (original) The system of claim 56 wherein the digital medium comprises a magnetic digital medium.

59. (previously presented) The system of claim 56 wherein the monitor monitors the transfer rate in real time, as the read. user data is transferred from the media reading device to the computing device

60. (previously presented) The system of claim 56 wherein the monitor monitors the transfer rate following transfer of the read user data from the media reading device to the computing device.

61. (original) The system of claim 56 further comprising and estimator for estimating the monitored data transfer rate and wherein the anomaly detector determines the presence of the anomaly region based on the estimated data transfer rate.

62. (previously presented) The system of claim 56 wherein the anomaly region causes a modification in the transfer rate of the read user data.

63. (previously presented) The system of claim 62 wherein the modification in the transfer rate results from the media reading device automatically initiating multiple retries of reading the

data symbols due the presence of the anomaly region.

64. (previously presented) The system of claim 62 wherein the modification in the transfer rate results from the media reading device automatically slowing down the reading of the data symbols due the presence of the anomaly region.

65. (previously presented) The system of claim 56 wherein the anomaly region is located at a predetermined location on the digital medium.

66. (previously presented) The system of claim 65 wherein the predetermined location comprises an absolute address on the digital medium.

67. (original) The system of claim 66 wherein the absolute address represents an encoded data value.

68. (previously presented) The system of claim 56 wherein the anomaly region is at a location on the digital medium that is analytically determined as a result of the step of determining the presence of the anomaly region.

69. (previously presented) The system of claim 68 wherein the predetermined location comprises an absolute address on the digital medium.

70. (original) The system of claim 69 wherein the absolute address represents an encoded data value.

71. (previously presented) The system of claim 56 wherein the anomaly region comprises a first anomaly region and wherein the anomaly detector further:

determines, from the monitored transfer rate, the presence of a second anomaly region on the digital medium corresponding to a second physical location of second data symbols on the digital medium; and

determines a relative location of the second anomaly region relative to the location of first anomaly region.

72. (original) The system of claim 71 wherein the authenticator further authenticates based on the determined relative location.

73. (previously presented) The system of claim 71 wherein the second anomaly region is located at a predetermined location on the digital medium.

74. (previously presented) The system of claim 71 wherein the second anomaly region is at a location on the digital medium that is analytically determined as a result of the step of determining the presence of the second anomaly region.

75. (original) The system of claim 71 wherein the relative location represents an encoded data value.

76. (previously presented) The system of claim 56 wherein the characteristic is the location of the anomaly region in the read user data, and wherein if the location of the anomaly region in the read user data matches the physical location of the anomaly region corresponding to the data symbols, then the digital medium is determined as authentic.

77. (previously presented) The system of claim 76 wherein if the location of the anomaly region in the read user data does not match the physical location of the anomaly region corresponding to the data symbols, then the digital medium is determined as non-authentic.

78. (previously presented) The system of claim 56 further comprising a controller for controlling user access to the user data read from the digital medium based on whether the digital medium is authentic.

79. (previously presented) The system of claim 78 wherein controlling comprises one of allowing access, disallowing access, and limiting access to the user data read from the digital medium.

80. (previously presented) The system of claim 56 wherein the determination of the presence of the anomaly region results from a difficulty in the reading of the read user data by a reading device.

81. (previously presented) The system of claim 56 wherein the anomaly region comprises a physical alteration of the digital medium that results in the user data corresponding to the anomaly region being transferred at a transfer rate that is different than a standard transfer rate of user data not corresponding to the anomaly region.

82. (original) The system of claim 81 wherein the physical alteration of the digital medium comprises a mechanical alteration.

83. (original) The system of claim 81 wherein the physical alteration of the digital medium comprises an optical alteration.

84. (original) The system of claim 81 wherein the physical alteration of the digital medium comprises a magnetic alteration.

85. (previously presented) The system of claim 56 wherein the authenticator resides in software code that is previously stored on the digital medium, prior to authentication.

86. (original) The system of claim 56 wherein the anomaly detector and authenticator reside in firmware that is stored in a media drive performing the authentication or reside in a computing device controlling the media drive.

87. (original) The system of claim 56 wherein a known characteristic of the anomaly region is previously stored, prior to authentication, and wherein authenticating the digital medium based on a characteristic of the anomaly region comprises comparing the characteristic to the known characteristic.

88. (canceled)

89. (previously presented) The system of claim 56 wherein the modification in the transfer rate comprises a reduction in the transfer rate and wherein the anomaly region is identified based on the extent of the reduction.

90. (previously presented) The system of claim 56 wherein the modification in the transfer rate comprises a reduction in the transfer rate to a resultant non-zero transfer rate.

91. (original) The system of claim 90 wherein the resultant non-zero transfer rate results in a determination that the anomaly region is a genuine anomaly region.

92. (previously presented) The system of claim 56 wherein the modification in the transfer rate comprises a reduction in the transfer rate to a resultant zero transfer rate.

93. (original) The system of claim 92 wherein the resultant zero transfer rate results in a determination that the anomaly region is a false anomaly region

94. (original) The system of claim 93 wherein the false anomaly region indicates that the

digital medium is non-authentic.

95. (previously presented) The system of claim 56 wherein the modification in the transfer rate comprises an increase in the transfer rate, and wherein the characteristic is determined based on the increase.

96. (previously presented) The system of claim 56 wherein the modification in the transfer rate comprises a response comprising an acceptable reduction in the user data transfer rate followed by a sudden increase in the transfer rate to an increased transfer rate that is greater than a maximum transfer rate.

97. (original) The system of claim 96 wherein the response indicates that an apparent anomaly region generated by an external source has been detected.

98. (original) The system of claim 97 further comprising a filter unit for filtering the apparent anomaly region such that authenticating is not based on the apparent anomaly region.

99. (original) The system of claim 56 wherein authenticating the digital medium is based on a characteristic of multiple anomaly regions.

100. (original) The system of claim 56 wherein authenticating the digital medium is based on multiple characteristics of the anomaly region.

101. (original) The system of claim 56 wherein the anomaly characteristic comprises anomaly severity.

102. (original) The system of claim 101 wherein the anomaly severity represents an encoded data value.

103. (previously presented) The system of claim 56 wherein the monitor further records prior settings of the media reading device prior to reading; and restores the prior settings of the reading device following authenticating.

104. (previously presented) The system of claim 103 wherein the monitor resets the media reading device, following recording of the prior settings.

105. (previously presented) The system of claim 104 wherein the monitor resets a cache on the media reading device is reset following recording of the prior settings.

106. (previously presented) The system of claim 103 wherein the monitor selects a data block size for the media reading device.

107. (previously presented) The system of claim 103 wherein the monitor disables excessive retry attempts by the media reading device.

108. (original) The system of claim 103 wherein the monitor reads locations of the digital medium known to be free of anomaly regions in order to achieve a maximum transfer rate.

109. (original) The system of claim 103 wherein the monitor ceases reading when an anomaly location has been encountered.

110. (previously presented) The system of claim 103 wherein the monitor stores the read user data for statistical analysis.

111. (previously presented) The method of claim 1 wherein monitoring the transfer rate of read user data from the media reading device to the computing device results from the reading of valid data stored on the digital medium.

112. (previously presented) The method of claim 56 wherein the transfer rate of read user data from the media reading device to the computing device that is monitored by the monitor results from the reading of valid data stored on the digital medium.